ORIGINAL

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	CC Docket No. 93-292
Policies and Rules	)	
Concerning Toll Fraud	)	

COMMENTS OF McCAW CELLULAR COMMUNICATIONS, INC.

E. Lee Kaywork
Corporate Vice President -
Revenue Requirements
Cathleen A. Massey
Senior Regulatory Counsel
McCaw Cellular Communi-
cations, Inc.
1150 Connecticut Ave., N.W.
Washington, D.C. 20036

R. Michael Senkowski
Katherine M. Holden
WILEY, REIN & FIELDING
1776 K Street, N.W.
Washington, D.C. 20006

Its Attorneys

January 14, 1994

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	CC Docket No. 93-292
Policies and Rules	)	
Concerning Toll Fraud	)	

COMMENTS OF McCAW CELLULAR COMMUNICATIONS, INC.

McCaw Cellular Communications, Inc. ("McCaw"), by its attorneys, hereby submits its comments with respect to the Notice of Proposed Rulemaking in the above-captioned docket.[1] The Commission's Notice represents an important step in the ongoing efforts of the telecommunications industry to prevent, detect, and successfully prosecute fraudulent use of telecommunications services and facilities. McCaw believes that the Notice will elicit a range of proposals that the Commission can use to structure a successful strategic attack on telecommunications fraud.

I. SUMMARY

Fraudulent use of services is a very serious problem confronting the cellular industry in particular and the telecommunications industry in general. As a result of the effects on its own operations, McCaw is an active participant in cellular industry efforts to develop responses to this threat. While cellular operators, like other

---

[1] FCC 93-496 (Dec. 2, 1993) ("Notice").

telecommunications carriers, must seek out available technical and usage solutions, there are steps that the Commission may take to enhance the likely success of these industry and private efforts.

There are a number of actions the Commission may pursue now, consistent with its statutory authority. Initially, the Commission must ensure that wireless carriers have and retain full rights to establish effective validation processes. A central element of any such process is the requirement that each subscriber unit have its own unique identification. Effective validation mechanisms are essential to billing integrity, efforts to combat fraud, and the conduct of surveillance at the behest of law enforcement agencies.

Moreover, the Commission should establish policies requiring that liability for fraud should be shared among all carriers whose facilities are compromised by the fraud, based on their ability to monitor and control access and/or validation. Allocation rules should give each carrier maximum incentive to take steps to prevent the occurrence of fraud.

In addition, other action may require enhanced or clarified grants of authority from Congress. First, the Commission, in cooperation with appropriate law enforcement representatives, should pursue legislation that clearly makes toll and cellular fraud a federal crime.

Second, the Commission should encourage carriers to cooperate with one another in investigating fraud. While the privacy rights of subscribers must be protected, carrier reluctance to share information in the absence of a subpoena hinders effective identification of fraud perpetrators. Legislation clarifying the respective rights and obligations of carriers and their customers with respect to information relevant to the investigation of possible fraudulent activities also may be useful. In addition, the Commission may be able to serve as a coordinating body to enhance the effectiveness of current investigative efforts.

Third, the Commission should ensure that it has all authority necessary to permit it to take action against non-regulated entities engaged in telecommunications fraud. A statutory amendment similar to the recent changes to Section 503 of the Communications Act, as amended, to permit the Commission to enforce its marking and lighting requirements against non-licensee tower owners, may be appropriate.

II. AS RECOGNIZED BY THE COMMISSION, FRAUDULENT USE OF CELLULAR PHONES IS A SERIOUS PROBLEM

The Notice recognizes that fraud has become a very serious problem in the telecommunications marketplace, with the industry and the Secret Service estimating annual losses of from one billion to five billion dollars (with total

annual industry billings of $175 billion).[2] With respect to the cellular industry specifically, the Notice accurately observes that "[t]he fraudulent use of cellular telephones has become a serious industry problem that results in financial losses to consumers, and increases the cost of doing business for the cellular industry."[3]

In McCaw's view, there are currently two categories of fraud unique to the cellular industry. First, "counterfeiting" or "cloning" is fraud perpetrated by stealing valid subscriber information to complete unauthorized calls. Specifically, a legitimately assigned electronic serial number ("ESN")/mobile identification number ("MIN") is programmed into another cellular phone on an unauthorized basis.[4] In many ways, the counterfeit phone is similar to the counterfeiting of credit cards.

Second, "tumbling" refers to the fraudulent user's alteration of the ESN or MIN before each call, either on a random or systematic basis.[5] Tumbling is usually accomplished by exploiting the cellular industry's typical billing and collection practices when a customer "roams" outside his or her home market.

---

[2] Notice at ¶ 4.

[3] Id. at ¶ 32.

[4] See id. at ¶ 33.

[5] See id.

When a subscriber "roams" -- that is, places cellular calls on another carrier's system -- carriers historically have permitted an authorized roaming customer's call to be completed while they search national databases to determine the validity of the ESN/MIN and associated account information. This process may take 15 to 30 minutes, or even longer. Until the carrier determines that the ESN/MIN is invalid, the cellular phone user is able to place calls.

By tumbling, a phone appears to the cellular system as a new roamer each time it places a call with a new ESN/MIN. The carrier is duped into completing a series of fraudulent roamer calls. Only later does the cellular carrier determine that there are no valid accounts associated with the ESN/MIN combinations and thus no known responsible subscribers. In this situation, the home carrier is the direct victim of the fraudulent activities.

In addition to the fraud that is unique to the cellular industry, cellular phones also may be used fraudulently in the same manner as landline handsets. Thus, for example, cellular service may be obtained on the basis of fraudulent subscriber information or pursuant to stolen credit card data.

McCaw, on its own and in conjunction with other cellular providers, has undertaken a number of efforts to combat cellular fraud. These activities include:

- Development of profiling capabilities that enable McCaw to monitor its cellular network and to detect fraud within 48 hours;
- Implementation of the National Cellular Network with pre-call validation, which eliminates the opportunities for tumbling fraud; and
- Active cooperation with local, state, and federal law enforcement agencies to apprehend and prosecute offenders.

Despite these efforts, however, fraud remains a very serious problem for the cellular marketplace.

Like other forms of telecommunications fraud, cellular fraud involves all of the carriers transporting the call. Obviously, the use of the cellular frequencies directly affects the cellular service provider. Since the vast majority of cellular calls are connected with a land-based telephone, they necessarily must traverse the landline network. As a result, the facilities of both local exchange carriers ("LECs") and interexchange carriers ("IXCs") are generally misused as well in the case of fraudulent cellular communications. The prevention and detection of fraudulent cellular usage thus necessarily requires cooperation among all the interconnected carriers.[6]

---

[6] Clearly all carriers desire to minimize unauthorized use of their networks. Where fraudulent use has occurred, however, the various carriers may have directly conflicting views about who bears the financial burden. Also, the various carriers may compete with one another in certain parts of the telecommunications marketplace, and may seek to use allocation of fraud liability as a competitive tool.

At present, McCaw and other members of the cellular industry do not require users to pay for electronic fraud. Thus, the charges associated with airtime used by counterfeit and tumbled phones are absorbed by the carrier.

Some cellular carriers also may absorb other charges stemming from the completion of fraudulent calls. McCaw, for example, resells interexchange service to its cellular subscribers. In the markets where this arrangement is in place, McCaw is responsible for the payment of the long distance charges associated with fraudulent calls. In contrast, in markets where the cellular carrier provides interexchange equal access, the cellular operator is responsible for the airtime charges, while the interexchange carrier absorbs the long distance charges.

Aside from the direct economic loss associated with fraudulent cellular calls, the usage patterns may affect system design and the installation of additional transmitter facilities. If fraudulent calls are concentrated in certain pockets of the carrier's coverage area, a cellular operator may be forced to add a new cell site or make other capital expenditures to expand system capacity to assure that legitimate customers can complete calls.

Cellular fraud, therefore, results in a direct loss of revenues, increases capital costs, and diverts resources from services for legitimate customers. While McCaw and other

carriers have expended considerable effort to combat fraud, the Commission is in a unique position to coordinate and support these initiatives.

III. WIRELESS SERVICES MUST EMPLOY EFFECTIVE VALIDATION PROCESSES TO INSURE BILLING INTEGRITY AND SUCCESSFUL ANTI-FRAUD PROGRAMS

Cellular carriers necessarily must have the ability to protect the integrity of the validation processes for the provision of service to subscribers. The key to an effective validation process is the premise that each cellular unit has its own, unique electronic serial number that in turn is associated with a particular mobile identification number. The Commission should take all steps necessary to protect the carrier's ability to uniquely identify a wireless unit.

Effective validation processes serve a number of critical goals. First, as illustrated in the discussion above about the nature of counterfeiting and tumbling, effective validation processes are essential in carriers' battles against fraud. Second, validation steps are necessary to permit the carrier to bill customers for use of the cellular and other facilities. Without the necessary information to determine the usage associated with particular units and particular accounts, cellular operators cannot economically operate their services.

Third, an absence of sound validation processes undercuts the ability of carriers to undertake appropriate surveillance on behalf of law enforcement agencies. Without unique unit information, carriers cannot guarantee that an ESN is associated with a single phone and cannot determine the location or identity of surveillance targets.

Given the importance of validation to these three critical activities, it would seem self-evident that a carrier's ability to assign a unique electronic identification number to each cellular phone should not be compromised. But recent events in the cellular marketplace show that the Commission needs to underscore the importance of effective validation and fashion additional enforcement tools to combat attempts to undermine cellular validation systems.

An example of an existing situation serves to illustrate these principles. A company known as C Two Plus Technology ("C2+") has developed a device known as the NAM Emulation Programming Device ("NEPD"). This device is used to create the equivalent of "cellular extension phones." Based on McCaw's understanding of the device's use, where the C2+ NEPD has been employed to modify a cellular telephone, multiple cellular phones will register with a cellular system as the

same unit.[7] The C2+ NEPD apparently does not physically alter the ESN of a cellular telephone phone, but instead somehow permits an override of a cellular phone's installed ESN with the ESN of another cellular telephone.

The Commission has indicated that the use of this device is impermissible under the Communications Act. In response to an inquiry about the C2+ NEPD, the Commission stated:

> It is a violation of Section 22.915 of the Commission's Rules for an individual or company to alter or copy the ESN of a cellular telephone. Moreover, it is a violation of the Commission's rules to operate a cellular telephone that contains an altered or copied ESN.[8]

---

[7] In addition to the implications for validation and fraud, the primitive technology utilized by entities such as C2+ significantly restricts customers' use of their phone. These multiple phones cannot roam, only one phone can receive calls, some cellular systems will automatically shut down all but one user with simultaneous origination, and the customer could be identified as a counterfeiter and have service abruptly terminated.

[8] Letter to Cellular Telecommunications Industry Association from John Cimko, Chief, Mobile Services Division (Jan. 15, 1993) ("FCC Letter"). This letter cited an earlier public notice that stated, inter alia, that "[p]hones with altered ESNs do not comply with the Commission's rules and any individual or company operating such phones or performing such alterations is in violation of Section 22.915 of the Commission's rules and could be subject to appropriate enforcement action." FCC Public Notice, "Changing Electronic Serial Numbers on Cellular Phones Is a Violation of the Commission's Rules," Rpt. No. CL-52-3 (Oct. 2, 1991). Section 22.915 of the Commission's Rules, entitled "Cellular system compatibility specification," provides that "[t]he technical specifications for compatibility of mobile and base station in the Domestic Public Cellular Radio Telecommunications Service are contained in the 'Cellular System Mobile Station-Land Station Compatibility

(continued...)

As the Commission has noted, its Part 22 rewrite proceeding contains a rule proposal relating to the technical specifications for mobile equipment to prevent unauthorized manipulation of the ESN.[9]

Despite the clear applicability of FCC restrictions to the C2+ device, C2+ has argued that its device is legal and is consistent with the public interest.[10] Regardless of the legitimacy or illegitimacy of C2+'s intent in developing and marketing the service, legitimate use of the phones created with the C2+ device cannot be distinguished from use of illegitimate counterfeit phones. The limited benefits associated with the "cellular extension phones" created by

---

[8](...continued)
Specification' (April 1981 Ed.), Office of Engineering and Technology Bulletin No. 53. This bulletin is contained in Appendix D to the Report and Order in CC Docket No. 79-318, and is printed in the Federal Register, of May 21, 1981." 47 C.F.R. § 22.915(a). Section 2.3.2, entitled "Serial Number" and as set forth in both the 1981 and 1983 editions of Bulletin No. 53, states: "The serial number is a 32-bit binary number that uniquely identifies a mobile station to any cellular system. It must be factory-set and not readily alterable in the field. The circuitry that provides the serial number must be isolated from fraudulent contact and tampering. Attempts to change the serial number circuitry should render the mobile station inoperative."

[9] See Notice at ¶ 34, citing In the Matter of the Commission's Rules Governing the Public Mobile Service, 7 FCC Rcd 3658, 3741 (1992) (notice of proposed rulemaking). The language of this proposed rule is clearly modeled on the existing OET cellular compatibility specifications document.

[10] Comments of C2+ Technology, Inc., CC Docket No. 92-115 (filed Apr. 20, 1993).

C2+ do not override the very serious opportunities for fraudulent use stemming from this technology.

C2+ has previously claimed that cellular carriers oppose its activities as a competitive threat that minimizes their revenues.[11] This characterization of operators' concerns, however, is not accurate. Rather, cellular providers like McCaw oppose the use of the C2+ NEPD and similar devices and technologies because they seriously compromise the cellular network and have the adverse consequences outlined above.

The Commission should take the opportunity provided by this proceeding to reiterate that activities like those involved with the use of the C2+ device are clearly prohibited by the Commission's existing rules. These activities undermine carrier operations and interfere with industry efforts to minimize fraud. These problems are a direct result of the fact that multiple cellular units share the same identifier.

Policies preserving the rights and abilities of cellular carriers to create appropriate validation procedures, with reliance on unique identification data for each cellular telephone, must be incorporated in the Commission's overall anti-fraud program. Further, the Commission should explicitly indicate that it will take all punitive action available to it against companies like C2+.

---

[11] See, e.g., id.

IV. McCAW ENDORSES THE BASIC CONCEPT OF SHARED CARRIER LIABILITY FOR FRAUD

McCaw believes that the Commission should adopt a shared liability model for the allocation of carrier responsibility for absorbing fraud. The guiding concept under this model is that carriers bear responsibility for the fraudulent use that they at least theoretically can control or where they would have a direct customer/carrier relationship with the user. McCaw expects that the parameters of this model will be defined during the course of this proceeding.

Existing arrangements in the cellular industry already reflect this basic theory. For example, McCaw discussed above the responsibility of various carriers for absorbing fraudulent long distance charges associated with cellular usage. In the equal access environment, both the cellular carrier and the IXC have opportunities to validate a call and monitor traffic and usage patterns because the user is a customer of each carrier. Accordingly, in that situation, in order to maximize each carrier's incentive to defeat and curb fraud, the long distance losses should be the responsibility of the IXC while the airtime losses are absorbed by the cellular carrier.

In contrast, where a cellular carrier resells interexchange services to its customers, the IXC has no direct relationship with the end user and has no opportunity

separately to validate the interexchange portion of the communications. Rather, only the cellular carrier is able to undertake call validation. In those situations, cellular carriers absorb both the airtime usage as well as the charges imposed by the IXC.

To the extent that identifying number information is passed along to any other carrier, such as a local exchange carrier, it too should be responsible for toll losses attributable to its transport of its customer's traffic.

Shared liability principles, as reflected in this example, are likely to ensure that all carriers whose facilities are involved in fraudulent calls have maximum incentives to deploy their own programs and to take other appropriate steps to ensure that fraud is minimized. The Commission should seek to maintain such arrangements where they already are in place, and extend the principles to other areas wherever feasible.

V. THE COMMISSION SHOULD PURSUE LEGISLATION TO ENHANCE THE PREVENTION, DETECTION, AND PROSECUTION OF FRAUD INVOLVING CELLULAR PHONES

The Commission has correctly recognized that current grants of authority may not provide the necessary tools for either the Commission or various enforcement agencies to prevent fraud, or to prosecute such activities when they do

occur.[12] While there are steps that the Commission and law enforcement agencies currently can take to deter toll fraud more effectively, McCaw believes that the Commission also should pursue a number of statutory changes, as detailed below.

A. Law Enforcement Agencies Need Improved Legal Tools To Enhance the Successful Prosecution of Cellular Fraud Perpetrators

As the Notice points out, "[t]he Department of Justice, local law enforcement agencies, and the U.S. Secret Service are among the agencies charged with the enforcement of criminal statutes."[13] Based on the record compiled in connection with its en banc hearing on toll fraud, the Commission has concluded that the existing federal statutes relied upon in the prosecution of toll and cellular fraud simply are not adequate to ensure necessary detection and prosecution.[14] McCaw believes that this finding mandates that the Commission answer in the affirmative the question raised in the Notice "whether to join with law enforcement authorities in encouraging Congress to enact legislation that clearly defines and penalizes this criminal activity and

---

[12] Notice at ¶ 12.

[13] Id. at ¶ 6.

[14] See id. at ¶ 12.

gives law enforcement the tools its needs to track and prosecute perpetrators of toll fraud."[15]

In seeking legislation, McCaw believes that the Commission should not seek to shift enforcement obligations to itself. The Commission simply does not have the resources to undertake the investigation and enforcement of toll fraud statutes. Instead, the Commission should continue to rely upon the existing federal and state agencies to enforce laws that clearly target the perpetrators of fraud in the telecommunications network. In addition, McCaw believes that the Commission should ensure that it has sufficient statutory authority to continue to act as a coordinator and facilitator among the different law enforcement bodies.

The statutory provision usually relied upon for toll fraud prosecutions at the federal level, 18 U.S.C. § 1029, clearly was enacted to cover types of fraud other than toll fraud.[16] While the statutory language has been interpreted to include "long distance telephone service access codes,"[17] there are other aspects of toll and cellular fraud that simply cannot be shaped to fall within the scope of the

---

[15] Id. at ¶ 13.

[16] See id. at ¶ 12.

[17] E.g., United States v. Brewer, 835 F.2d 550 (5th Cir. 1987).

statutory prohibitions.[18] The telecommunications industry and its customers would be best served by statutes that clearly render toll and cellular fraud activities criminal violations subject to straightforward prosecutions at the federal level.[19]

The statutory language could take the form of an amendment to Section 1029 of Title 18 specifically to encompass telecommunications fraud. While the legislation should address known fraudulent activities, it should be broadly worded to encompass new fraud technologies and techniques.[20]

---

[18] Indeed, the Tenth Circuit Court of Appeals recently has ruled that Section 1029 does not encompass tumbling within its prohibitions. United States v. Brady, No. 93-4085, slip op. (Dec. 21, 1993).

[19] The Notice observes that "[t]he Secret Service estimates that as few as thirteen states have enacted statutes specifically dealing with telephone fraud crimes." Notice at n.28. Consistent with its efforts to coordinate the activities of various entities in combatting toll fraud, the Commission also may want informally to urge all states to enact appropriate legislation prohibiting fraudulent telecommunications activities.

[20] As the Notice pointed out, as detection methods are developed in one area of fraudulent behavior, new techniques are implemented. See Notice at ¶ 12. Thus, the statutory definitions necessarily must be very expansive in order to avoid containing loopholes that can be readily abused by the perpetrators of fraud.

B. The Commission Also Should Pursue Necessary Statutory Changes To Facilitate the Ability of Different Carriers To Cooperate in the Investigation of Potential Fraudulent Use of Cellular Phones

As discussed above, cellular fraud involves communications paths over facilities provided by cellular carriers, LECS, and IXCs. Thus, detection of the perpetrators of fraud necessarily involves cooperation among these different carriers.

McCaw's experience, however, is that carriers often do not readily or successfully cooperate in promptly investigating situations where the patterns of telecommunications usage suggest that fraudulent activity is underway. For example, one of the McCaw cellular companies might determine that several different counterfeit cellular phones are placing calls to one landline telephone number. This circumstance would suggest to the cellular carrier that fraudulent behavior may be occurring involving the landline customer. But, if McCaw approaches the appropriate landline carrier about a joint investigation of the situation, or to obtain information that may be turned over to law enforcement agencies, McCaw often confronts an unwillingness to cooperate.

McCaw recognizes that telephone service subscribers have legitimate privacy concerns. Moreover, most carriers (including McCaw) necessarily act very conservatively with

respect to requests for information from other carriers as well as law enforcement agencies about their subscribers. Thus, carriers often require that they be served with a subpoena before disclosing information about a customer's telephone number, usage, or other specific information. These practices, however, generally hinder successful detection and prosecution of fraudulent activities.

McCaw believes that the privacy concerns of subscribers and the interests of carriers in minimizing telecommunications fraud can be more effectively balanced. Specifically, at present, a law enforcement agency might issue a subpoena only to a cellular carrier in order to obtain the records necessary to investigate possible fraud. Only later, after unsuccessful efforts by the cellular carrier and/or the law enforcement agency to obtain information from other carriers involved in the communications transmission, is a second (or third) subpoena issued to other involved carriers. This delay often provides the fraud perpetrator with a window of opportunity permitting it to escape detection. In effect, operators of fraudulent services can take effective advantage of the dilemma of inter-carrier cooperation in order to escape identification and prosecution.

Because time often is of the essence in investigating possible fraud, the Commission should urge all carriers to

cooperate to the maximum extent permitted by law in the collection and analysis of information. In addition, the Commission should take what steps it can to facilitate the expedited, concurrent issuance of subpoenas to all carriers with information relevant to a particular investigation, in lieu of the current piecemeal approach.

The Commission also should determine, in cooperation with the responsible law enforcement agencies, whether statutory changes should be sought to assist in achieving successful inter-carrier cooperation in connection with the investigation of possible fraudulent activities. Clarification of the rights and responsibilities of carriers might enable them to respond more effectively to requests to assist in collecting information for an investigation, without interfering with the legitimate privacy rights of members of the public.

Similarly, adoption of shared liability principles, as discussed below, will increase the incentives of carriers to undertake cooperative investigations. In that event, such investigations would no longer aid only interconnected service providers but might also serve to reduce a carrier's own financial exposure.

C. The Commission Should Pursue Legislation Necessary To Permit It To Extend Appropriate Restrictions to Non-Regulated Entities

In connection with its request for comment on the nature of the measures the Commission should consider taking in connection with cellular fraud, the Notice cites Section 503(b)(5) of the Communications Act of 1934, as amended, 47 U.S.C. § 503(b)(5), which provides for "forfeiture proceedings against non-licensees or non-applicants who willfully or repeatedly violate the Commission's rules."[21] McCaw believes that this statutory provision (or others) must be strengthened to ensure that the Commission does have all authority necessary to permit it to enforce toll fraud safeguards against entities that are not otherwise subject to regulation by the Commission. Clarification of the authority of the Commission to take appropriate enforcement action against non-regulated entities such as C2+, similar to the statutory grant of authority recently given to the Commission to act with respect to non-licensee owners of towers supporting communications transmitters, may enhance the alternatives available to the Commission to ensure that the rules and policies mentioned above are followed in all respects.

---

[21] Notice at n.54.

VI. CONCLUSION

The Notice in this proceeding represents an important step in the efforts to control the rapidly increasing levels of fraudulent use of telecommunications facilities. While customers and carriers bear much responsibility, there are a number of steps, outlined in the comments above, that the Commission can take to facilitate the successful deterrence and prosecution of telecommunications fraud. McCaw urges the Commission to act promptly and in a considered fashion to take all steps feasible to minimize fraudulent use of cellular and other telecommunications facilities.

Respectfully submitted,

McCAW CELLULAR COMMUNICATIONS, INC.

By: Cathleen A. Massey

E. Lee Kaywork
Corporate Vice President -
Revenue Requirements
Cathleen A. Massey
Senior Regulatory Counsel
McCaw Cellular Communications, Inc.
1150 Connecticut Ave., N.W.
Washington, D.C. 20036
(202) 223-9222

By: Katherine M. Holden

R. Michael Senkowski
Katherine M. Holden
WILEY, REIN & FIELDING
1776 K Street, N.W.
Washington, D.C. 20006
(202) 429-7000

Its Attorneys

January 14, 1994